UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/627,927	07/28/2000	Michael John Sabin	ATMSP-003	2434

7590 09/21/2004

Kenneth D'Alessasndro
Sierra Patent Group Ltd
Post Office Box 6149
Stateline, NV 89449

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/627,927	**Applicant(s)** SABIN, MICHAEL JOHN	
	Examiner Christopher A. Revak	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 July 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,26,32,39,40,46,47,54,67 and 68* is/are rejected.

7)☒ Claim(s) *2-25,27-31,33-38,41-45,48-53, and 55-66* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *see attached*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on July 24, 2002 is in compliance with the provisions of 37 CFR 1.97. The examiner has considered the information disclosure statement.

Claim Objections

2. Claim 46 is objected to because of the following informalities: It is recited of "private key parameters defined by the parameters {seed,}", it appears that there should be an additional value for the parameter besides just a seed since there is a comma and parameters is referred to in plural from. Did the applicant intend to include another parameter value or is the parameter value just a seed? Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1,26,32,54,67, and 68 are rejected under 35 U.S.C. 102(b) as being anticipated by Quisquater et al.

As per claim 1, it is disclosed by Quisquater of a RSA box (containing a processor and nonvolatile memory space operatively coupled to the processor), using the Chinese Remainder Theorem, that includes a set of private key parameters utilizing less storage space than a full parameter set {p, q, d sub p, d sub q, v} and provides better computational efficiency than the minimal parameter set {p, q} wherein the private key can be recovered from the set of stored private key parameters (see page 1, column 1).

As per claim 26, it is disclosed by Quisquater that a set of private key parameters are defined by parameters {p, q, v} wherein p and q are given prime factors of a public modulus, and v is derived from pv mod q = 1 (see page 1, column 1).

As per claim 32, Quisquater discloses of a set of private key parameters defined by the parameters {p, q} wherein p and q are prime factors of a public modulus (see page 1, column 1).

As per claim 54, Quisquater discloses of cryptosystem private key recovery device that includes a RSA box (containing a processor and nonvolatile memory space operatively coupled to the processor), using the Chinese Remainder Theorem, that includes a set of private key parameters utilizing less storage space than a full parameter set {n, d} and provides better computational efficiency than the minimal parameter set {p, q}(see page 1, column 1).

As per claim 67, it is taught by Quisquator of a method for recovering a private key whereby private key parameters are stored in a RSA box (containing memory space), using the Chinese Remainder Theorem, utilizing less storage space for the private key parameters than the full parameter set {p, q, d sub p, d sub q, v} and providing better computational efficiency than the minimal parameter set {p, q}(see page 1, column 1).

As per claim 68, Quisquator discloses of a method for recovering a private key whereby private key parameters are stored in a RSA box (containing memory space), using the Chinese Remainder Theorem, utilizing less storage space for the private key parameters than the full parameter set {n, d} and providing better computational efficiency than the minimal parameter set {p, q}(see page 1, column 1).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 39,40,46, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Quisquater in view of Zhang, U.S. Patent 6,154,541.

As per claim 39, Quisquater discloses of private key parameters wherein v is derived from pv mod q = 1 (see page 1, column 1). The teachings of Quisquater are silent in disclosing of the use of a seed value derived from a random number generator. Zhang discloses of use of a seed value from a random number generator (column 21, lines 46-54). It would have been obvious to a person of ordinary skill in the art at the time of the invention to be motivated to apply a random number generator for generating a seed value in order to protect in the integrity of the private key. Zhang recites motivation for use of a seed value generated by a random number generator by disclosing if a seed is not known, it is hard to learn the sequence of numbers that are used to generate it (column 21, lines 54-55). It is obvious that the teachings of Quisquater would have benefited from the teachings of Zhang for using a seed value generated by a random number generator that is used for key generation.

As per claim 40, Quisquater is relied upon for use of a RSA box (containing a processor) that calculates p and q (see page 1, column 1). The teachings of Zhang are relied upon for use of a seed to be used for private keys (includes values p and q), please refer to the recited motivation as is recited above for use of a seed value.

As per claim 46, the teachings of Quisquater are silent in disclosing of the use of a seed value derived from a random number generator. Zhang discloses of use of a seed value from a random number generator (column 21, lines 46-54). It would have been obvious to a person of ordinary skill in the art at the time of the invention to be motivated to apply a random number generator for generating a seed value in order to protect in the integrity of the private key. Zhang recites motivation for use of a seed value generated by a random number generator by disclosing if a seed is not known, it is hard to learn the sequence of numbers that are used to generate it (column 21, lines 54-55). It is obvious that the teachings of Quisquater would have benefited from the teachings of Zhang for using a seed value generated by a random number generator that is used for key generation.

As per claim 47, Quisquater is relied upon for use of a RSA box (containing a processor) that calculates p and q (see page 1, column 1). The teachings of Zhang are relied upon for use of a seed to be used for private keys (includes values p and q), please refer to the recited motivation as is recited above for use of a seed value.

Allowable Subject Matter

7. Claims 2-25,27-31,33-38,41-45,48-53, and 55-66 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As per claims 2,7,13,19,27,33,41,48, and 55, the claims were found to be allowable based on the subject matter if incorporated into the corresponding independent claims.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Please see attached PTO-892

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843 until October 20, 2004 and can then be reached at 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached at 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131
9/15/04

CR
September 15, 2004